CBTC 시스템 개발을 위한 시스템엔지니어링과 안전성 분석의 통합

Integration of Systems Engineering and System Safety Analysis for Developing CBTC System

박중용[1], 박영원[2]

Joong-Yong Park, Young-Won Park

Keywords : *model-based systems engineering, system safety analysis, CBTC(Communications-Based Train Control)*

Abstract

This article proposes an integrated systems engineering and safety analysis model for safety-critical systems development. A methodology in system design for safety is considered during the early phase of the development life cycle of systems engineering process. The evolution of the design automation technology has enabled engineers to perform the model-based systems engineering. A Computer-Aided Systems Engineering(CASE) tool, CORE, is utilized to integrate the systems engineering model with a system safety analysis model. The results of the functional analysis phase can drive the analysis of the system safety. An example of Communications-Based Train Control(CBTC) system for an Automated Guided Transit(AGT) system demonstrated an application of the integrated model.

1. 서 론

2차 세계 대전을 겪으면서 엔지니어들은 그 전에는 겪어 보지 못 했던 복잡한 시스템들을 개발해야 하는 상황에 직면했다. 그 당시의 새로운 시스템들은 구성 부품 수가 많았고, 복잡하면서 인간과의 인터페이스를 갖는 반자동화 시스템이었으며 입력에 대한 출력을 예측하기 힘든 특징을 가지고 있었다[1]. 1970년대와 1980년대를 거치면서 컴퓨터의 활용성이 높아져 시스템은 더 거대하고 복잡해졌으며, 칩이 중요한 구성 부품이 되었다[2]. 또한, 컴퓨터를 구동시키는 소프트웨어의 비중 역시 점점 커지게 되었다. 하드웨어와 소프트웨어가 혼합되어 있는 현대의 시스템은 상당수가 반자동화 또는 자동화 시스템이기 때문에 안전성의 측면에서 철저한 검증이 필요하다. 즉, 철저한 안전성 분석을 통해 요구사항을 검증하고 필요하다면 수정해서 설계에 반영해야만 구축된 시스템이 의도된 거동을 보일 수 있기 때문이다.

시스템 엔지니어링은 시스템의 획득자 및 기타 이해당사자로부터 요구사항을 추출한 후 이를 규격서로 전환시켜 요구사항을 만족시키는 시스템을 개발하게끔 하는 정형화된 절차, 방법 및 도구를 망라하는 것이다. 시스템 엔지니어링은 일반적으로 최초 요구사항을 시스템 요구사항, 부품 요구사항 등 하향식으로 할당한 후 다시 규격화된 요구사항에 부합되는지를 검증하며 부품에서부터 시스템으로 상향식으로 통합하는 'Vee' 모델을 채택하고 있다[3]. 'Vee' 모델은 시스템 엔지니어링뿐만 아니라 소프트웨어 공학 분야에서도 널리 활용되고 있다.

경량전철 시스템과 같은 대형 복합기술 시스템은

1 아주대학교 대학원 시스템공학과, 박사과정

2 정회원, 아주대학교 대학원 시스템공학과, 정교수

구성하고 있는 컴포넌트 및 인터페이스, 시스템의 기능, 그리고 자동화 운영 등의 시스템 요구사항들이 방대하고 복잡하다. 이러한 경량전철 시스템의 요구사항 관리, 기능 분석, 물리적 아키텍쳐 구축과 같은 시스템엔지니어링 업무를 전산지원도구를 사용하여 수행하는 모델기반 시스템엔지니어링의 방법론과 결과를 이미 보여준바 있다[4]. 이와 같은 방법론은 경량전철시스템 뿐만 아니라 차세대 고속전철 시스템에도 적용되어 좋은 성과를 거두기도 했다[5].

한편, 경량전철 시스템은 대표적인 안전필수적 시스템(safety-critical system)이기 때문에 철저한 안전성 분석을 필요로 한다. 즉, 안전성 분석을 통해서 내재된 위험요소들을 식별하고 위험을 제거하거나 줄이기 위해 안전 요구사항을 규격서에 반영하는 작업이 필요하다. 안전성 분석은 개발하고자 하는 시스템의 개발 단계에 따라 각기 다른 방법이 적용된다. 즉, 개념설계 단계에는 아직 물리적 컴포넌트에 대한 구체적인 데이터가 없기 때문에 기능 위주로 안전성 분석이 수행되고 상세설계 단계에서는 상대적으로 풍부한 데이터가 확보되므로 실제 부품 위주로 안전성 분석이 수행된다. 안전성 분석의 방법으로는 FFA(Functional Failure Analysis), FMEA(Failure Modes and Effects Analysis), FTA(Fault Tree Analysis)가 주로 쓰인다[6].

시스템엔지니어링과 안전성 분석을 통합하려는 연구는 일부 학자들에 의해 제한적으로 수행되어 왔다. Papadopoulos는 시스템 개발 초기부터 계층적으로 안전성 분석을 수행하는 모델을 개발했는데 여기서 변형된 FFA를 제시하고 FTA를 자동적으로 그릴 수 있는 알고리즘을 개발하였다[6]. Robinson은 철도의 신호 시스템 설계 도구를 개발하였는데 기능 요구사항으로부터 규격서를 뽑아내고 안전성 원리에 위배되지 않는지 검증하는 기능을 제공하였다[7]. 또한, Johannessen은 소프트웨어 공학에서 주로 사용하는 쓰임새 다이아그램(Use case diagram)을 활용하여 안전성을 분석하는 방안을 제시하였다[8].

본 논문에서는 제품 개발의 초기 단계에서 수행하는 안전성 분석을 시스템엔지니어링과 통합하여 실시하는 방법론과 결과를 소개하였다. 개발 초기에 실시하는 안전성 분석의 전제 조건은 시스템의 기능이 정확하게 식별되어야 한다는 것이다. 그러나, 국내의 실정은 개념설계에 기술적 활동을 집중하지 않다 보니 기능분석이 제대로 되지 않아 안전성 분석이나 고장분석이 부품 단위 수준에서만 일부 수행될 뿐이었다. 이번 연구에서는 이러한 국내 실정을 타개하기 위해 시스템 개발 초기에 CASE(Computer-Aided Systems Engineering) 도구 중의 하나인 CORE를 사용해서 시스템엔지니어링과 안전성 분석을 통합하여 수행하는 방안을 제시하였다. 하나의 모델 안에 시스템엔지니어링 모델과 안전성 분석 모델이 통합되어 있으므로 안전성을 고려한 시스템 규격서를 효율적으로 작성할 수 있다.

2. 시스템엔지니어링과 안전성 분석

2.1 시스템엔지니어링

시스템엔지니어링은 계층적 구조를 따라 고객의 요구사항으로부터 규격서를 만들어내고 완성된 제품이 규격서를 만족하는지 확인해나가는 프로세스이다. 이러한 프로세스를 Fig. 1의 'Vee' 모델이 보여주고 있다[3].

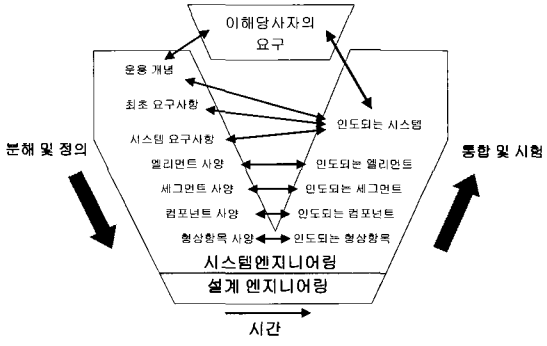

Fig. 1 'Vee' model of systems engineering

Fig. 1에서 분해 및 정의로 표현되어 있는 부분에서 규격서가 만들어지는데 각 단계는 요구사항 분석, 기능 분석/할당, 아키텍쳐 설계, 그리고 시스템 분석/통제로 이루어진 시스템엔지니어링 핵심 프로세스에 의해 수행된다[4]. 네 가지 업무는 반복되며 수행되는 특징을 가지고 있다. 그리고, 그림에서 수평 화살표들은 '검증(verification)' 관계를, 그 외의 화살표들은 '논증(validation)' 관계를 표현하고 있다.

현대에 이르러 컴퓨터의 발달로 전산지원도구가 활발히 이용되면서 모델기반의 시스템엔지니어링이 가능하게 되었다[4]. 특히, 기능 분석의 경우 정적인 분

석만이 아니라 동적 분석이 CASE 도구의 발달로 수월하게 이루어지게 되었다.

2.2 안전성 분석

시스템의 안전성 역시 시스템엔지니어링과 마찬가지로 제2차 세계 대전 이후에 엔지니어링의 한 분야로 인정받기 시작했다. 1970, 1980년대를 거치면서 컴퓨터 기술의 발전은 시스템의 안전에 대한 개념을 많이 바꾸어 놓았다. 특히, 마이크로프로세서의 등장으로 컴퓨터뿐만이 아니라 일반 기계에도 칩이 사용되면서 상당수의 장치들이 반자동, 또는 자동화되었으며, 소프트웨어가 시스템의 핵심 부분으로 자리잡게 되었다. 1950년대 이후 이미 복잡해지기 시작했던 시스템들은 칩과 소프트웨어들이 구성 요소로 삽입되면서 그 복잡도가 더 커지고 있다. 특히, 소프트웨어의 경우는 자체의 고장이 문제되는 것이 아니고 잘못된 거동이 문제가 되어 시스템 수준에서 철저한 요구사항과 기능 분석이 수행되어야 한다는 주장이 제기되었다[1]. 즉, 시스템엔지니어링 프로세스를 통한 해석 결과들을 가지고 안전성을 분석해야 하는 것이다. 이와 같이 시스템엔지니어링의 산출물이 안전성 분석과 결합되면서 시스템 개발 초기부터 안전성에 대한 고려가 이루어지기 시작했다. CENELEC EN 50128, DEF STAN 00-55, IEC 61508, MIL-STD-882D와 같이 안전성 분석에 대한 표준이 군이나 각 산업계에서 발표되었는데 그 중, 미국의 국방부에서 발간한 MIL-STD-882D에서 제시한 안전성 분석의 절차는 다음과 같다[9].

1) 시스템 안전성 접근법에 대한 문서화
2) 위험(hazards) 요소 식별
3) 재해(mishap) 리스크 평가
4) 재해 리스크 경감 지표 식별
5) 허용 가능 수준으로 재해 리스크 감소시키기
6) 재해 리스크 감소의 검증
7) 관련 당국에 의한 위험 요소의 검토 및 잔여 재해 리스크의 수락
8) 위험 요소, 위험 요소의 종결, 잔여(residual) 재해 리스크 추적

개발 초기 주로 많이 사용되는 안전성 분석의 방법으로는 기능 FTA(Fault Tree Analysis)와 HAZOP (Hazards and Operability Analysis), FFA (Functional Failure Analysis) 등이 있다.

3. 통합 모델

통합 모델은 CASE 도구인 CORE를 사용해서 기능 분석의 결과를 안전성 분석에 활용하고 다시 안전성 분석의 결과를 피드백하여 기능 분석을 수행할 수 있도록 하는데 그 목적이 있다. 물론 기능 분석이 개선되면서 필요에 따라 안전 요구사항을 포함한 시스템 요구사항도 수정된다. 본 논문에서는 통합 모델의 근간이 될 기능 분석, 아키텍쳐 설계와 안전성 분석의 기법을 선정하고 각각의 분석을 수행하되 이 과정에서 식별된 기능과 컴포넌트를 활용하여 안전성 분석을 수행할 수 있는 틀을 구축했다.

3.1 시스템엔지니어링

CASE 도구인 CORE를 활용해서 수행하는 모델기반 시스템엔지니어링의 모델은 Fig. 2와 같다. 즉, 2장에서 다루었던 시스템엔지니어링 활동을 CORE에서 수행함으로써 공통된 데이터베이스에 시스템의 설계 자료를 축적할 수 있는 것이다. 요구사항, 기능, 아키텍쳐의 각 요소들은 ERA(Element, Relation, Attribute) 데이터 모델을 기반으로 연결되어 추적성을 확보할 수 있다는 특징을 가지고 있다.

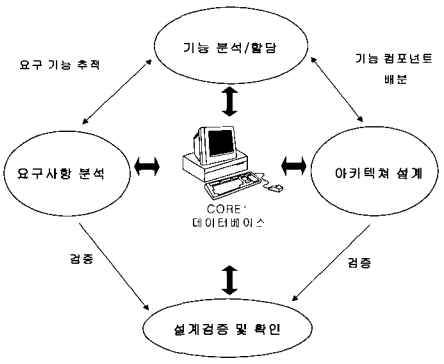

Fig. 2 Model of systems engineering using CORE

요소(Element)는 요구사항, 기능과 같이 시스템엔지니어링을 수행하는데 필요한 것들로 각 요소들은 적절한 속성(Attribute)을 가지며 다른 요소들과 관계(Relation)를 가지고 있다. 그러한 관계를 Fig. 3에서 보여주고 있다. 문서, 요구사항, 기능, 컴포넌트, 쟁점

사항 등이 요소이며, 화살표로 표시되어 있는 incorporates, allocated to등이 관계이다. 여기서 쟁점사항은 각 요소에 대한 문제점이 발견되었을 경우 그것의 변경 이력 및 결정사항을 기록하기 위해 생성하는 요소이다.

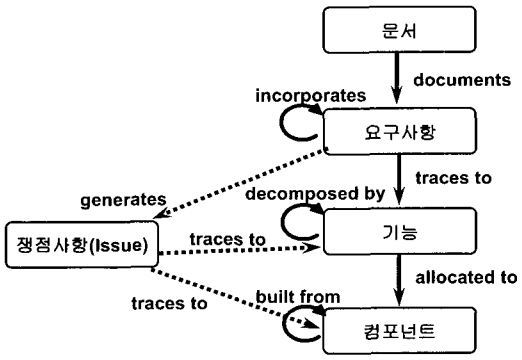

Fig. 3 The relations of elements in CORE

이러한 ERA 구조를 활용하게 되면 시스템엔지니어링에서 사용하는 기본 요소들뿐만 아니라 안전성 분석과 관련된 기본 요소들을 만들어 관계를 부여함으로써 시스템엔지니어링 결과물과 안전성 분석 결과물을 연결할 수 있게 된다. 이것이 통합 모델의 기본 이론이다. 한편, 안전성 분석과 시스템엔지니어링을 통합하는데 있어서 중요한 단계는 기능 분석이다. 식별된 기능을 안전성 측면에서 분석하는 것이 안전성 분석이기 때문이다. 기능 분석은 시스템의 시나리오를 작성하고 시나리오를 바탕으로 FFBD(Functional Flow Block Diagram)를 구축하는 단계로 수행되었다. FFBD는 시뮬레이션을 통해 논리적 검증을 마치게 된다.

3.2 안전성 분석

제품의 개발 단계에 따라 적용되는 안전성 분석 방법은 모두 다르다. 본 연구에서는 개발 초기에 적용하는 안전성 분석을 다루었으므로 주로 기능 수준에서 위험을 식별하게 된다. 그러한 방법들로 대표적인 것은 HAZOP, FFA, FTA 등이 있다. 그 중에서 본 논문에서는 기능 분석 결과를 그대로 활용할 수 있는 FFA를 채택하여 분석을 수행하였다. FFA는 시스템엔지니어링 업무를 수행하면서 작성된 FFBD를 기본으로 주요 기능이 제대로 수행되지 못 했을 때 전체 시스템에 어떤 영향을 끼치는지 파악하는 방법이다. FFBD를 보면 문제가 되는 기능과 입력 및 출력 관계를 가지면서 연결되어 있는 기능이 있고, 추적성을 확보한 데이터 덕분에 그 기능과 연결된 컴포넌트를 즉각 확인할 수 있기 때문에 FFA 작업을 수월하게 진행할 수 있는 것이다. 본 연구에서는 하나의 기능이 수행되면서 산출되는 출력 아이템(인터페이스가 된다)이 다른 기능을 구동시키는 입력 아이템이 된다는 것에 착안하여 아이템에 고장이 발생하는 상황을 가정하여 FFA를 수행하였다. HAZOP 역시 FFA와 유사하게 분석이 진행되지만, 소프트웨어와 칩이 내장되어 있는 시스템의 고장 분석을 수월하게 할 수 있도록 안내어(guide word)를 제시한다는 점에서 차이가 있다[10]. CORE는 CASE 도구이기 때문에 시스템엔지니어링을 수행하기 위한 요소, 관계, 속성 등은 제공하지만 안전성 분석에 대한 틀은 제공하지 않는다. 따라서, 통합 모델을 구축하기 위해서 안전성 분석을 위한 요소, 관계, 속성 등을 새로 구축하였으며 이들과 시스템엔지니어링 데이터간의 관계도 설정하였다. 안전성 분석까지 고려해서 개발한 모델은 Fig. 4와 같다.

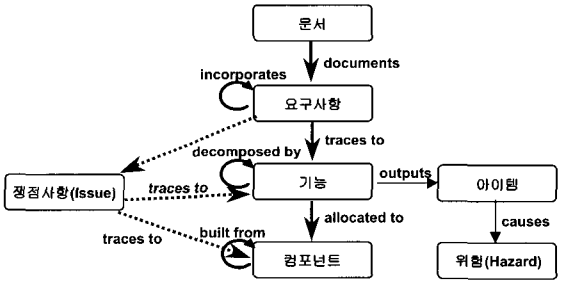

Fig. 4 Integrated model of systems engineering and safety analysis

안전성 분석을 통해 식별되는 위험들을 처리하는 과정은 기본적으로 리스크 분석 과정과 동일하다. 이는 위험 요인들 역시 리스크의 한 대상이기 때문이다. 모델을 보면 기능이 산출하는 아이템이 표현되어 있고 이 아이템이 제대로 산출되지 않았을 경우 발생가능한 위험이 아이템에 causes 라는 관계를 통해 연결되어 있음을 알 수 있다. 위험 요소의 속성으로는 고장 원인, 고장 영향, 심각도 등이 첨가된다.

4. 적용 예: CBTC 시스템

4.1 CBTC 시스템

열차의 신호 시스템은 안전성의 측면에서 또는 운용 효과성의 측면에서 꾸준히 개선되어 왔다. 경량전철 시스템에서는 열차의 운행 안전거리 간격을 가능한 단축하는 것이 중요하다. 간격을 줄이기 위해서는 열차의 위치를 정확하게 감지하는 것이 선행되어야 한다. 선행 열차의 위치와 속도가 정확히 인지되면 후행 열차는 불필요한 감속을 하지 않게 되고 따라서 지연을 막을 수 있는 것이다. 종래의 신호시스템은 지상의 궤도 회로를 기본으로 열차의 위치를 지상에서 인지한 후 열차의 진행을 결정하여 차상으로 전달하였다. 하지만, 열차 검지의 단위가 수백 미터에서 수 킬로미터이고 수 비트의 용량을 가지는 제어 신호로는 적절한 제어를 수행하기가 어려웠다. 또한, 제어장치가 지상에 설치되면서 대량의 케이블로 연결되어 막대한 전력과 보수를 필요로 한다. 이와 같이 종래의 시스템은 열차를 보호하는데는 효과적이지만 하부구조물을 이용하는데 있어서는 효율적이지 못하다는 제약사항을 가지고 있다. 이러한 제약사항을 극복하여 지상의 인프라를 되도록 작게 하고 차상에 지능화된 설비를 도입하는 방안이 고려되어 대안으로 제시된 시스템이 CBTC 시스템이다[11].

CBTC 시스템의 특징은 다음과 같다.

1) 궤도 회로와 관계없이 높은 정밀도를 가지고 열차의 위치를 결정할 수 있다.

2) 기존의 시스템 보다 월등하게 많은 제어와 상태 정보를 전달할 수 있는 연속적인 지상-차상 및 차상-지상 간 데이터 통신 네트워크를 구비하고 있다.

3) 열차의 상태 및 제어 데이터를 처리하고 연속적인 자동열차보호(ATP: Automatic Train Protection) 기능을 제공하는 지상 및 차상의 핵심 처리기를 구비하고 있다. 또한 자동열차운행(ATO: Automatic Train Operation)이나 자동열차감시(ATS: Automatic Train Supervision) 기능도 필요에 따라 제공된다.

이와 같은 세 가지 주요 기능을 포함하는 CBTC 시스템의 전반적인 기능 구성이 Fig. 5에 표현되어 있다[12].

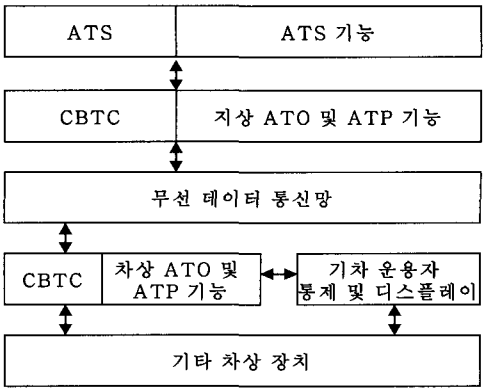

Fig. 5. Top level functional block diagram of CBTC

4.2 기능 분석

Table 1 The scenario of train position decision

언제	주어	부터/에게	무엇을	어떻게	동사
시간 1	열차위치결정기능		열차제어 지역진입		인식한다
시간 2	Global Positioning	무선 데이터 통신망	탐지 데이터	무선	수신한다
시간 2	Global Positioning		열차위치		결정한다
시간 3	Global Positioning	데이터 베이스	열차위치 정보		저장한다
시간 4	열차위치추적기능	데이터 베이스	열차위치 정보		불러온다
시간 5	열차위치추적기능		열차위치		추적한다
시간 6	열차위치추적기능	열차관리기능	열차위치 정보		보낸다
시간 6	열차위치추적기능	데이터 베이스	열차위치 정보		저장한다

본 연구는 세 가지 주요 기능(ATP, ATO, ATS) 에 대해 각각 시나리오를 작성한 후 FFBD를 그리고, 세 가지를 통합하여 전체 CBTC 시스템의 거동을 분석하는 방법으로 진행되었다. Table 1은 ATP 기능 중에서 열차의 위치를 결정하는 시나리오를 작성한 예이다.

작성된 시나리오를 바탕으로 FFBD를 그리면 Fig.

6과 같다. 그림에서 네모로 표현된 것이 기능이며 각이 둥근 네모는 각각의 기능에 대한 입/출력 데이터나 정보들로서 아이템이라는 요소이다. 이것은 기능 인터페이스를 표현한다.

4.3 안전성 분석

CBTC 시스템에서 예측되는 중요 고장 모드로 다음과 같이 여섯 가지를 선정하였다.

1) CBTC 역 컴퓨터 고장
2) CBTC 차상 컴퓨터 고장
3) 무선 데이터통신 네트워크 고장
4) 트랜스폰더 인터페이스 고장
5) 연동장치 인터페이스 고장
6) 플랫폼 도어 인터페이스 고장

여섯 가지 고장 모드 중에서 CBTC 역 컴퓨터와 차상 컴퓨터의 고장에 대해 FFA를 수행했으며 그 결과를 통합 모델에 구축하였다. 본 절에서는 CBTC 역 컴퓨터의 고장이 시스템에 어떤 영향을 주는지에 대한 분석 과정과 결과를 소개한다.

CBTC 역 컴퓨터는 ATP 역 컴퓨터라고도 불리는데 역에 설치되어 주로 ATP 기능을 수행한다. CBTC 역 컴퓨터가 전체 CBTC 시스템 아키텍처에서 어떤 위치인지 Fig. 7에서 확인할 수 있다. CBTC 시스템이 역, 열차, ATS 컴퓨터로 나뉘어져 있고, CBTC 역 컴퓨터는 역의 하부 컴포넌트 9개중의 하나임을 알 수 있다.

Fig. 8은 CBTC 역 컴퓨터가 수행하는 기능이 무엇인지 파악할 수 있는 그림으로 CORE에서 제공하는 추적성 파악 기능의 우수성을 볼 수 있다. 즉, CBTC 역 컴퓨터에 고장이 발생했을 때 수행할 수 없는 기능을 일목요연하게 파악할 수 있다. 개발 초기에 수행한 분석이라 이러한 하부 기능들을 수행하는 컴포넌트들은 식별되지 않았으나 기능의 고장만 예측되면 이에 대처할 수 있는 설계가 가능하다.

Fig. 6 FFBD of train position decision

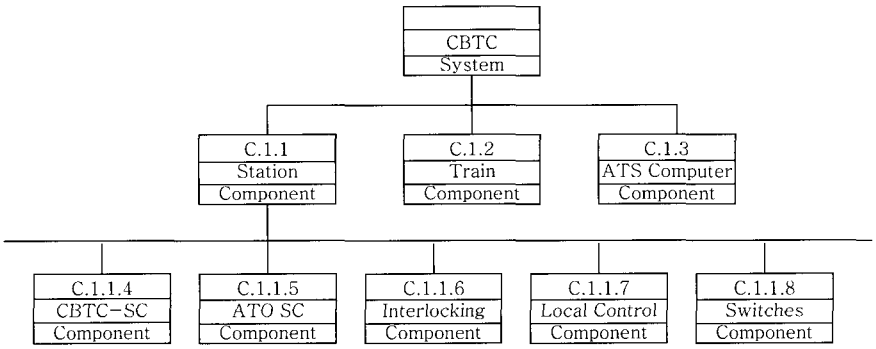

Fig. 7 The architecture of CBTC system

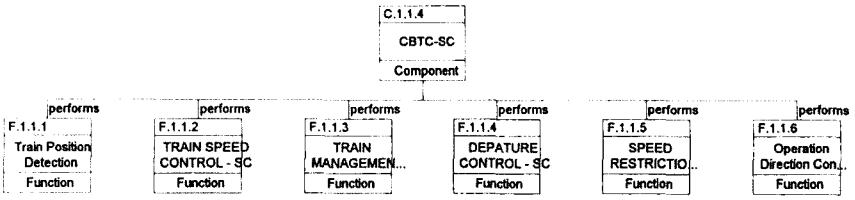

Fig. 8 The functions of CBTC station computer

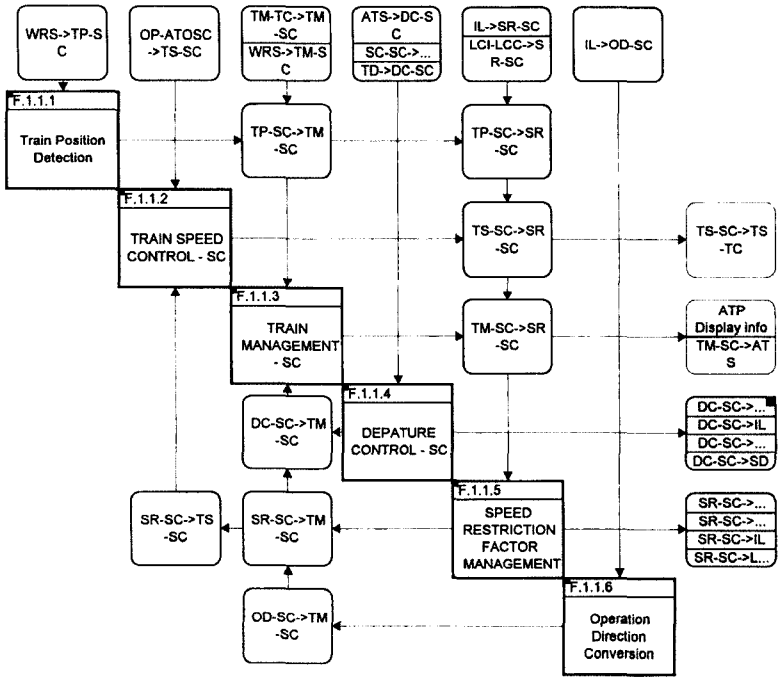

Fig. 9 N² chart

Fig. 9는 CBTC 역 컴퓨터가 다른 컴포넌트와 공유하는 인터페이스를 쉽게 확인할 수 있는 N^2 차트이다. CBTC 역 컴퓨터에 고장이 발생했다는 의미는 출력이 제대로 산출되지 않음을 의미하며 그 출력을 입력으로 하는 다른 컴포넌트에 영향을 미칠 것이다.

작성된 그림과 데이터를 토대로 'CBTC 역 컴퓨터'의 기능에 의해 산출된 아이템들을 식별하고 이 아이템들이 제대로 송신되지 않을 때 시스템에 미치는 영향을 분석하였다. Table 2가 FFA의 결과이다. 여기서 심각도는 MIL-STD-882D에서 제시된 고장의 심각도에 대한 네 가지 분류[9]를 채택하여 결정하였다.

Fig. 10은 요구사항, 기능, 컴포넌트, 아이템, 그리고 위험간의 추적성이 잘 나타난 그림으로 위와 같이 각 요소간의 추적성을 보여주는 그림을 CORE에서는 자동으로 생성한다. Fig. 11은 Table 2의 아이템 중에서 '제한상태' 아이템이 송신되지 않았을 때 발생하는 위험 요소의 고장영향과 심각도에 대한 데이터가 표현되어 있는 CORE의 작업 창을 보여주고 있다.

Table 2 The results of FFA

아이템	고장형태	고장영향	심각도
열차위치	송신되지 않음	ATO 기능 마비	치명적
안내정보	송신되지 않음	속도관리불가	치명적
제동명령	송신되지 않음	열차 추돌	치명적
열차검지 정보	송신되지 않음	열차 추돌	치명적
ATP표시 정보	송신되지 않음	연동기능마비로 인한 열차 추돌	치명적
주행시작	송신되지 않음	열차출발지연	중요하지않음
문닫음	송신되지 않음	열차출발지연	중요하지않음
제한상태	송신되지 않음	사고위험증대	중요함
속도제한 요소	송신되지 않음	연동기능마비로 인한 열차 추돌	치명적

이번 FFA에서 고장 원인은 분석하지 않았다. 개발단계가 더 진행되면서 CBTC 역 컴퓨터의 하부 컴포넌트 들이 식별되어야 가능하기 때문이다. 다만, 하드웨어의 고장, 소프트웨어의 거동 분석 실패와 같은 원인을 짐작하는 것은 가능하다. 하지만, 고장 영향 분석만을 통해서도 CBTC 역 컴퓨터는 ATP 기능의 수행을 위한 주요 장치임을 인정할 수 있다. 그러므로 고장 방지(fail-safe) 원리에 따라 구현되고 설계되어야 하는 바이탈 기능이 CBTC 역 컴퓨터에 대해 필요하다.

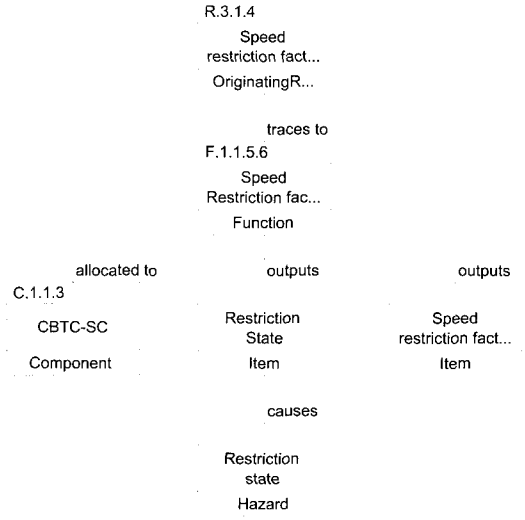

Fig. 10 Traceability of systems engineering data

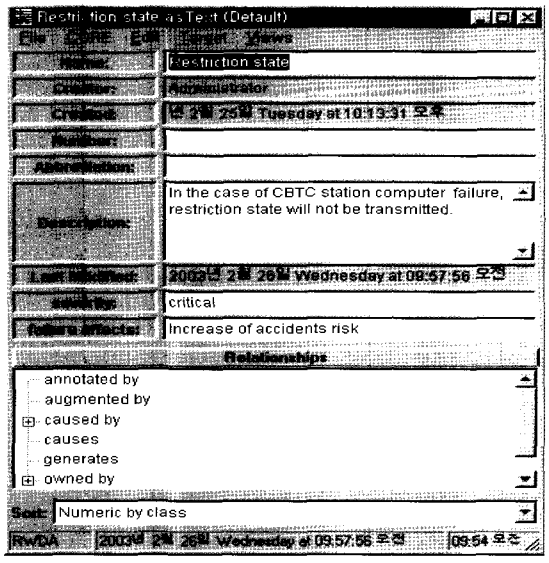

Fig. 11 Window of Hazard element

5. 결 론

시스템 안전성 분석을 시스템엔지니어링 작업과 연계하여 수행할 수 있게 도와주는 통합 모델을 제시하

였다. 이러한 통합모델은 시스템 수준의 설계대안들이 제시되기 전에 안전성 문제를 파악하고 이해하기 때문에 안전성이 우선적으로 고려된 설계해법들을 식별케 하는 매우 중요한 장점을 제공한다. 국내의 실정은 시스템엔지니어링을 하는 업무가 널리 퍼져 있지 않기 때문에 안전성 분석의 기초 데이터가 되는 기능 분석 결과가 제대로 산출되지 않고 있다. 또한, 안전성 분석도 시스템 차원에서의 접근보다는 하부 컴포넌트 위주의 접근을 통해 주로 수행되어 왔다. 따라서 안전성 필수적 시스템들의 설계 구현에 뒤늦게 소극적인 대처만이 가능하게 된다. 하지만, 시스템엔지니어링과 안전성 분석은 서로 밀접한 관련을 가지고 있는 엔지니어링 분야이기 때문에 두 분야에서 도출되는 결과들을 통합하여 관리해야 안전한 시스템을 초기단계부터 개발할 수 있게 된다. 본 논문에서는 통합의 당위성을 제시하는 측면에서 기능 분석의 결과를 직접 안전성 분석에 적용해서 피드백을 얻는 방법론과 모델을 제시하였다. 이로써 시스템의 요구사항, 기능, 컴포넌트, 그리고 위험 요소들이 모두 추적성을 가지고 구축되는 모델을 확보하게 되었다. 특히, 경량전철 시스템의 CBTC 시스템과 같은 안전필수적 시스템에 대해 본 모델을 적용해 봄으로써 복잡한 시스템의 안전성을 향상시킬 수 있는 효과적인 방법임을 입증하였다. CASE 도구를 직접 개발하지 않고 CORE를 선택한 이유는 시스템엔지니어링 전산지원도구로 상용화된 도구들이 거의 CORE와 같은 ERA 구조를 채택하고 있고, 널리 사용되고 있으며, 구조상 응용의 가능성이 무척 크기 때문이다.

향후에는 현 모델을 바탕으로 실제 위험 요소를 CORE에 구축하여 데이터를 통합하고, HAZOP, FMEA와 같은 다른 안전성 분석 방법을 적용한 모델을 추가할 계획이다. 또한, 요소와 속성, 관계를 보강하여 FFA와 같은 안전성 분석의 결과가 좀 더 가시적으로 표현될 수 있도록 할 계획이다. 장기적인 연구 과제로는 인적 요소가 포함되거나 다중 고장을 표현할 수 있는 안전성 분석 모델을 개발하여 이를 시스템엔지니어링 모델과 통합하는 일이다.

후 기

본 연구는 "경량전철시스템 기술개발사업" 연구 결과의 일부로서 건설교통부의 지원으로 수행되었습니다.

참 고 문 헌

1. N. G. Leveson, "Safeware : System Safety and Computers", Addison-Wesley Publishing Company, Inc., Boston, 1995.
2. N. Storey, "Safety-Critical Computer Systems", Addison-Wesley Publishing Company, Inc., Harlow, 1996.
3. D. M. Buede, "The Engineering Design of Systems", John Wiley & Sons, Inc., New York, 2000.
4. 박중용, 박영원, "모델기반 시스템공학을 응용한 대형복합기술 시스템 개발", 제어.자동화.시스템공학 논문지,제 7 권, 제 8 호, pp. 689-696, 2001.
5. 유일상, 박영원, "차세대 고속전철 시스템 엔지니어링 체계 모델 개발", 한국철도학회지, 제 4 권, 제 4 호, pp. 147-154, 2001.
6. Y. Papadopoulos, J. McDermid, R. Sasse and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure", Reliability Engineering and System Safety, vol. 71, issue. 3, pp. 229-247, 2001.
7. N. Robinson, P. Kearney and D. Tombs, "Automatic Generation and Verification of Design Specifications for Railway Signalling Applications", Proc. of the 11th Annual INCOSE Symposium, 2001.
8. P. Johannessen, C. Grante, A. Alminger, U. Eklund and J. Torin, "Hazard Analysis in Object Oriented Design of Dependable Systems", Proc. of The International Conference on Dependable Systems and Networks, pp. 507-512, 2001.
9. DOD, "MIL-STD-882D: Standard Practice for System Safety", Department of Defense, United States of America, 2000.
10. Ministry of Defence, "Defence standard 00-58 : HAZOP Studies on Systems Containing Programmable Electronics", Ministry of Defence, Great Britain, 2000.
11. IEEE, "IEEE P1474.1/D8.0 Draft Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements", Institute of Electrical and Electronics Engineers, Inc., New York, 1999.
12. 한국철도기술연구원, "경량전철시스템 기술개발사업 3차년도 연구결과보고서 (분야: 신호제어시스템기술개발)", 건설교통부, 2001.